# Annual 47 C.F.R. § 64.2009(e) CPNI Certification EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2011

Date filed: February 23, 2012

Name of company covered by this certification: Mayerick Media of Eau Claire Communications, LLC

Form 499 Filer ID: 824210

Name of signatory: Paul A. Banks

Title of signatory: CFO

I, Paul A. Banks, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company complies with the Commission's CPNI rules. See 47 C.F.R. § 64,2001 et seq.

The company's procedures, namely not using, disclosing or permitting access to CPNI, is in compliance with the requirements set forth in Section 64,2001 et seq. of the Commission's rules. A copy of the company's Statement of Compliance is attached hereto as EXHIBIT A.

The company has not taken any action (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year. CPNI of the company is held in a secure location with access limited to senior officers of the company.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

The company represents and warrants that the above certification is consistent with 47 C.F.R. § 1.17 which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Paul A. Banks, CFO

Maverick Media of Eau Claire

Communications, LLC

#### STATEMENT OF COMPLIANCE

The operating procedures of Maverick Media of Eau Claire Communications, LLC ("Maverick") ensure compliance with the FCC's CPNI Rules. Such procedures are as follows:

### 1. Use of CPNI in Marketing

- a. Maverick does not use CPNI in any of its marketing efforts, and does not permit the use of, or access to, customer CPNI by our affiliates or any third parties. We use, disclose or permit access to CPNI only for the purposes permitted under 47 U.S.C. Sections 222(c)(1) and (d).
- b. Maverick has implemented a system by which the status of a customer's CPNI approval can be clearly established prior to the use of CPNI. Each customer's record contains a designation identifying whether or not we have obtained, through the processes permitted by the FCC's rules, the customer's approval to use, disclose or permit access to his or her CPNI.

#### 2. <u>CPNI Safeguards</u>

- a. Maverick has designated a compliance officer to maintain and secure the company's CPNI records and to supervise training of all company employees.
- b. Maverick trains it personnel as to when they are, and are not, authorized to use or disclose CPNI, and Maverick has an express disciplinary process in place if rules are violated.
- c. Maverick authenticates the identity of a customer prior to disclosing CPNI based on customer-initiated telephone contact or in-store visit.
- d. Maverick discloses call detail information ("CDI") in a customer-initiated call only: at the customer's request, by sending the CDI to the customer's address of record; or by calling back the customer at his or her telephone number of record.
- e. Maverick discloses CPNI to a customer in person at our retail location(s) only when the customer presents a valid photo ID and the ID matches the name on the account.

## 3. CPNI Recordkeeping and Reporting

- a. Maverick is prepared to provide the FCC with written notice, within five business days of any instance where the "opt out" mechanisms do not work properly.
- b. Maverick is prepared to notify the U.S. Secret Service and FBI within seven business days after the occurrence of an intentional, unauthorized (or exceeding authorization), access to, use of, or disclosure of CPNI. Maverick may also notify the customer of such breach, after consulting with the investigatory agency(ies), if it is believed there is an extraordinarily urgent need to notify a customer (or class of customers) in order to avoid immediate or irreparable harm. Maverick will notify the customer of the breach after seven business days following notification to the FBI and Secret Service, if such agencies have not requested that we postpone disclosure to the customer.
- c. Maverick will maintain records of any discovered breaches, notices to the Secret Service and FBI, and their responses, for at least two years.